REMARKS

Claims 62-72 have been amended. Claims 1-6, 8-31, 33-47 and 49-72 are pending in the application. Reconsideration is respectfully requested in light of the following remarks.

Section 101 Rejection:

The Examiner newly rejected claims 62-72 under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Specifically, the Examiner asserts that claims 62-72 for disclose a carrier medium. Applicants traverse this rejection. However, to expedite prosecution, claims 62-72 have been amended to recite a "computer-readable, storage medium comprising program instructions." Removal of the § 101 rejection is respectfully requested.

Section 102(a) Rejection:

The Examiner rejected claims 1, 2, 8-13, 15-17, 20, 21 and 23-26, 27, 28, 33-36, 38-43, 47, 49-51, 56-59, 61-63, 66, 67, 69, 70 and 72 under 35 U.S.C. § 102(a) as being clearly anticipated by Adams (U.S. Patent 6,718,470). Applicants respectfully traverse this rejection for at least the reasons below.

Regarding claim 1, contrary to the Examiner's assertion, Adams fails to disclose determining client capabilities for a client, where the client capabilities are capabilities of the first service that the client is permitted to use. Adams teaches a system for granting security privileges by providing test criteria data so that matching security privilege certificates (or other authorization credentials) may be selected from among multiple subscriber privilege data. Adams teaches that certificates, such as Kerberos tickets, privilege attribute certificates, or other public key certificates (Adams, column 7, lines 48-55) may be selected from among multiple privilege data based on test criteria supplied by a relying unit (such as a software application, computer node or other

entity). A selector entity may search a common repository of security privilege certificates. The selector entity then returns any and all privilege data that meets the test criteria data. Thus, the selector unit may return multiple certificates, each of each meets the test criteria data. (see, Adams, column 3, lines 26-59; column 4, lines 25-36; and column 5, lines 18-46). However, Adams fails to mention anything about determining the client's capabilities, where the client capabilities are capabilities of the first service that the client is permitted to use.

The Examiner cites column 6, lines 49-61 and specifically refers to Adams' centralized privilege data selector. Additionally, **in the Examiner's Answer**, the Examiner argues that Adams' "centralized privilege data selector determines the capabilities of [a] subscriber by using the subscriber's identification to retrieve attribute certificate associated with the subscriber" (Examiner's Answer, page 13, lines 11-11). **However, the Examiner's interpretation of Adams is incorrect. Adams does not describe his privilege data selector as determining client capabilities.** Instead, Adams teaches that the privilege data selector selects among subscriber privilege data "based on the privilege test criteria data." The Examiner's cited passage does not describe *determining a client's capabilities*. Instead, the cited passage only refers to how Adams' privilege data selector selects among privilege data for a plurality of subscribers. As noted above, Adams teaches that his data selector selects privilege data that meets test criteria data supplied by the relevant relying party. Adams' teaches that privilege data "may be any suitable data required by a relying party to facilitate, for example, acceptance, granting or access decision[s] related to a subscriber unit or user of a subscriber unit" (Adams, column 3, lines 35-38). Adams gives as examples of privilege data, "data representing a user position in a company" and "transaction signing limits" (Adams, column 3, lines 38-41). The type of privilege data used in Adams' system and selected by the privilege data selector clearly fails to represent client capabilities that are capabilities of a service that the client is permitted to use, as recited in claim 1.

Thus, the privilege data selector does not determine a client's capabilities, but instead only compares the potential privilege data, such as a user's position in a company,

to the supplied test criteria data. Nowhere does Adams mention determining a client's capabilities where the client capabilities are capabilities of the first service that the client is permitted to use.

Further in regard to claim 1, Adams also fails to disclose binding the client capabilities to the authentication credential. The Examiner cites column 6, lines 65-66 and argues that the matching attributes are sent as pre-qualification data. However, the matching attributes referred to in the cited passage are the authentication credentials (such as Kerberos tickets, privilege attribute certificates or other public key certificates) and are not bound to any client capabilities. Nowhere does Adams mention binding determined client capabilities to an authentication credential.

In the Examiner's Answer the Examiner cites column 6, line 65 to column 7, lines 2 and again asserts that Adams' matching attributes certificates are sent as pre-qualification data. **However, the cited passage only states that any attribute certificates matching the test criteria data are sent as pre-qualification privilege data back to the subscriber unit.** Adams also teaches that after the subscriber unit sends the pre-qualification privilege data to the relying unit, the relying unit performs a pre-qualification privilege verification to ensure that the supplied attribute certificates do indeed meet the test criteria data. Adams' system uses test criteria data and pre-qualification privilege data to avoid having clients sending unnecessary privilege information. When sending pre-qualification privilege data, Adams' system does not bind any client capabilities to an authentication credential.

Furthermore, Adams clearly teaches that the matching attribute certificates are obtained from an attribute certificate repository and returned as pre-qualification privilege data. Adams does not mention anything about binding anything with the attribute certificates, which the Examiner considers the authentication credential of claim 1. Sending matching attribute certificates and verifying that they match certain test criteria data does not have anything to do with binding client capabilities to an authentication credential.

Additionally in regard to claim 1, Adams fails to disclose the service using the authentication service to authenticate the authentication credential received in the message from the client. The Examiner cites column 7, lines 3-8 where Adams teaches that after the subscriber unit sends pre-qualification privilege data to the relying unit, the relying unit performs a pre-qualification privilege verification to ensure that the supplied attribute certificates do indeed meet the test criteria data. The Examiner also argues, "the relying party uses the centralized privilege data selector to generate credential for authentication." However, generating an authentication credential is not the same as using an authentication service to authenticate an authentication credential obtained from the authentication service by a client and sent to the service, as recited in claim 1.

Furthermore, the cited passage does not support the Examiner's statement. Instead, the cited passage states that the relying party unit performs the pre-qualification privilege verification and sends a confirmation message back to the subscriber unit. However, the pre-qualification privilege verification does not involve the relying unit using the central privilege data selector, which the Examiner equates to the authentication service of claim 1, to perform the verification. Adams teaches that the pre-qualification privilege verification involves comparing the test criteria data with the pre-qualification privilege data (e.g. the attribute certificates) "to see if they are consistent." Adams' system involves the relying unit verifying that the attribute certificates actually meet the test criteria data. Contrary to the Examiner's assertion, nowhere does Adams state that the privilege data selector is used as part of this verification.

In the Examiner's Answer, the Examiner cites column 6, line 61 to column 7, line 9 and refers to Adams' pre-qualification privilege data being generated by the authentication service/centralized privilege data selector "so that it can be verified by the first service/relying party." The Examiner further asserts, "thus, the first service uses the authentication service to authenticate subscribers based [ ] to grant[ing] access to subscribers." **However, as noted above, Adams' relying unit receives the pre-qualification privilege data from the centralized privilege data selector and then**

compares the test criteria data with the pre-qualification privilege data **as a pre-qualification privilege verification, which the Examiner considers authenticating an authentication credential. Adams clearly teaches that the relying unit performs this comparison on its own. Thus, the relying unit only receives the pre-qualification privilege data from the privilege data selector. It does not use the privilege data selector to perform the pre-qualification privilege verification, which the Examiner considers authenticating an authentication credential.**

Anticipation requires the presence in a single prior art reference disclosure of each and every limitation of the claimed invention, arranged as in the claim. M.P.E.P 2131; *Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co.*, 221 USPQ 481, 485 (Fed. Cir. 1984). The **identical** invention must be shown in as complete detail as is contained in the claims. *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). As discussed above, Adams clearly fails to disclose determining client capabilities for a client, where the client capabilities are capabilities of the first service that the client is permitted to use, binding the client capabilities to the authentication credential, and the service using the authentication service to authenticate the authentication credential received in the message from the client. Therefore, Adams clearly cannot be said to anticipate claim 1.

For at least the reasons above, the rejection of claim 1 is not supported by the prior art and removal thereof is respectfully requested. Similar remarks also apply to claims 27, 43, 51 and 62.

Regarding claim 2, Adams fails to disclose a client obtaining an address for the authentication service from an advertisement for the service, wherein accessing the authentication service includes the client sending a message to the address for the authentication service requesting the authentication credential to use the advertised service.

The Examiner cites FIG. 5 and column 6, lines 31-40 of Adams. However, the cited portions make no mention of a client obtaining an address for the authentication service from an advertisement for the service. Instead, the cited passage describes one embodiment of Adams' system in which the relying party sends privilege test criteria data to a centralized privilege data selector and in which a subscriber sends identification information to the centralized privilege data selector. The data selector then returns to the subscriber all attribute certificates from a certificate repository that meet the received test criteria data. The subscriber then transmits the returned certificates to the relying unit. Nowhere does Adams describe a client obtaining an address for the authentication service from an advertisement for the service.

In the Examiner's Answer, the Examiner also cites column 5, lines 14 – 17 and column 6, lines 49-51. The Examiner also asserts, "in order for the subscriber to request authentication credential, the subscriber must be informed of the authentication service's address as well as the first service's address." Thus, the Examiner's reasoning is that since Adams' subscriber sends a privilege verification request to the privilege data selector the website must include the address of the privilege data selector. **However, the teachings of Adams do not support the Examiner's conclusion.** Instead, the Examiner is merely speculating regarding the workings of Adams' system.

Firstly, at the Examiner's cited passage, Adams states that the subscriber unit may communicate a request to a website of the relying party, which the Examiner equates to the service of Applicants' claim, to request "access to another application controlled by the relying party" (Adams, column 5, lines 13-17). Adams does not mention anything about the website including an address for the privilege data selector, which the Examiner equates to the authentication service of Applicants' claims. Secondly, the cited passage that mentions the website is part of a larger passage describing as example system in which the privilege data selector is actually on the subscriber unit. For instance, Adams states, "subscriber unit 200, such as a software application, network node, or other suitable mechanism for communicating with another subscriber of relying party, *has a privilege data selector 104* in the form of an attribute certificate selector 202" (italics

added, Adams, column 4, lines 58 – 62). Thus, in the example system described by Adams at the Examiner's cited passage, the privilege data selector is part of the subscriber unit. Thus, the subscriber unit would not require an address for the privilege data selector to be included in the website relied upon by the Examiner. Additionally, it would not make any sense for the "website of the relying party" to include an address for a privilege data selector on the subscriber unit.

At the Examiner's other cited passage where Adams' described another example system in which the privilege data selector is separate from the subscriber unit, Adams makes no mention of a website. Without some specific teaching by Adams that the subscriber unit obtains the address to the centralized privilege data from a service advertisement, Adams cannot be said to anticipate a client obtaining a service advertisement for a service, where the service advertisement includes an address for an authentication service, as recited by Applicants' claim.

For at least the reasons above, the rejection of claim 2 is not supported by the cited art and removal thereof is respectfully requested. Similar remarks also apply to claims 13, 28, 52, and 63.

Regarding claim 9, Adams fails to disclose that determining client capabilities includes the client accessing an access policy service to obtain a capability token indicating which capabilities of the service the client is permitted to access. The Examiner cites column 6, lines 31-67. The cited passage describes use of a centralized privilege data selector in Adams' system. Adams teaches that a relying unit communicates privilege test criteria data to the centralized privilege data selector and that a subscriber unit sends privilege verification request data including subscriber identification data and selected relying party identification data to the centralized privilege data selector. The centralized privilege data selector uses the subscriber identification data to obtain the appropriate attribute certificates from an attributes certificate repository and uses the relying party identification data to obtain the correct privilege test data for the identified relying party unit. However, the cited passage does

not mention a client accessing an access policy service to obtain a capability token indicating which capabilities of the service the client is permitted to access. Adams' centralized privilege data selector sends attribute certificates that match the privilege test data to the subscriber unit.

In the Examiner's Answer, the Examiner argues that Adams' "pre-qualification privilege data includes the capabilities of the service that the subscriber is permitted to access." **However, the Examiner's interpretation of Adams is incorrect.** Nowhere does Adams mention a client obtaining a capability token indicating which capabilities of the service the client is permitted to access. Adams attribute certificates include such certificates as Kerberos tickets, DCE PAC, etc. that do not indicate which capabilities of a service the client is permitted to access. Additionally, Adams states that the privilege data "may be data representing a user position in a company (e.g., an employee or independent contractor), transaction signing limits, or other suitable data" (parenthesis in original, Adams, column 3, lines 38-41). Thus, Adams' privilege data, including pre-qualification privilege data, does not refer to capabilities of a particular service that a subscriber is permitted to access, as asserted by the Examiner.

Thus, for at least the reasons above, the rejection of claim 9 is not supported by the cited art and removal thereof is respectfully requested. Similar remarks also apply to claim 34,

Regarding claim 11, Adams fails to disclose where determining client capabilities is performed by the service. The Examiner cites column 6, lines 17-20 and refers to the sending of privilege test criteria data to a subscriber unit by a relying unit. However, the sending of privilege test criteria data is not the same as determining client capabilities. Instead, Adams describes that the privilege test criteria indicates the specific privilege information necessary for the relying part to grant privilege to a subscriber unit (Adams, column 3, lines 47-51). For example, Adams describes privilege test criteria data indicating data representing a required membership or indicating the public key

certificates that the relying unit would consider for authentication purposes (Adams, column 5, lines 37-40 and column 7, lines 47-55). Thus, the relying unit, which the Examiner equates to the service of Applicants' claims, does not perform the determining of client capabilities, but instead provides privilege test criteria data indicating what types of privilege data it would recognize or consider before granting the subscriber unit privilege.

The rejection of claim 11 is not supported by the cited art and removal thereof is respectfully requested.

Regarding claim 12, Adams fails to disclose the client generating a message gate for accessing the service, where the message gate sends request message from the client to the service to access the service and where the message gate includes the authentication credential **in each message** to the first service. The Examiner cites column 6, line 67 – column 7, line 8 of Adams. However, the cited passage makes no mention whatsoever regarding a client generating a message gate or about the message gate including an authentication credential in each message to the service. The cited passage merely states that Adams' subscriber unit sends pre-qualification attributes or privilege data to the relying unit "through a suitable communication link". However, merely stating that the pre-qualification attributes are sent through a suitable communication link does not disclose the specific limitations of generating a message gate or about a message gate including an authentication credential in each message to the service. Nowhere does Adams mention anything regarding either message gates or about including an authentication credential in each message to the first service.

In the Examiner's Answer, the Examiner also cites column 4, lines 10-11 and column 6, line 67 – column 7, line 2. At the first cited passage (column 4, lines 10-11) Adams states that his FIG. 1 illustrates "an example of a system for granting security privilege 100 that may be applied to a communication system employing cryptography based security." The second cited passage (column 6, line 67 – column 7, line 2) Adams

states that the subscriber unit transmits the pre-qualified attributes or privilege data to the relying party unit through a suitable communication link. The Examiner argues, "[s]ince the communication is encrypted and the pre-qualification privilege data [is] transmitted to the relying party when requesting a service, thus a message gate is generated and the authentication credential [is] included in each message to the first serviced." **However, the fact that the subscriber unit sends the pre-qualification privilege data to the relying unit does not imply that the pre-qualification privilege data, which the Examiner equates with the authentication credential of Applicants' claim, is embedded *with every message* from the subscriber unit to the relying unit.** Adams' system involves using privilege data as part of granting the subscriber unit access to some other application on the relying party. For example, Adams states that after a subscriber unit is granted privilege, "[t]he subscriber unit may then access the relying party". Thus, Adams' subscriber unit clearly sends other messages to the relying party. However, Adams does not that the pre-qualification privilege data is embedded *in every message* sent from the subscriber unit to the relying unit.

Thus, for at least the reasons above, the rejection of claim 12 is not supported by the cited art and removal thereof is respectfully requested. Similar remarks also apply to claim 36.

Regarding claim 13, Adams fails to disclose the client obtaining a service advertisement for the first service before accessing the first service, where the service advertisement includes an address for the authentication service and an address for the first service. The Examiner cites column 6, lines 31-48. However, this passage does not disclose a client obtaining a service advertisement. Instead, as described above regarding claims 2 and 9, this passage describes a centralized privilege data selector that receives information from a subscriber unit and a relying unit. However, the subscriber unit, which the Examiner equates to the client of Applicants' claim, does not obtain any service advertisement. Adams fails to mention anything about a service advertisement that includes an address for the authentication service and an address for the first service.

In the Examiner's Answer, the Examiner also cites column 5, lines 14 – 17 and column 6, lines 49-51. The Examiner also asserts, "in order for the subscriber to request authentication credential, the subscriber must be informed of the authentication service's address as well as the first service's address." Thus, the Examiner's reasoning is that since Adams' subscriber sends a privilege verification request to the privilege data selector the website must include the address of the privilege data selector. **However, the teachings of Adams do not support the Examiner's conclusion.** Instead, the Examiner is merely speculating regarding the workings of Adams' system.

As described above regarding claim 2, Adams states that the subscriber unit may communicate a request to a website of the relying party, which the Examiner equates to the service of Applicants' claim, to request "access to another application controlled by the relying party" (Adams, column 5, lines 13-17). Adams does not mention anything about the website including an address for the privilege data selector, which the Examiner equates to the authentication service of Applicants' claims. Secondly, the cited passage that mentions the website is part of a larger passage describing as example system in which the privilege data selector is actually on the subscriber unit. For instance, Adams states, "subscriber unit 200, such as a software application, network node, or other suitable mechanism for communicating with another subscriber of relying party, *has a privilege data selector 104* in the form of an attribute certificate selector 202" (italics added, Adams, column 4, lines 58 – 62). Thus, in the example system described by Adams at the Examiner's cited passage, the privilege data selector is part of the subscriber unit. Thus, the subscriber unit would not require an address for the privilege data selector to be included in the website relied upon by the Examiner. Additionally, it would not make any sense for the "website of the relying party" to include an address for a privilege data selector on the subscriber unit.

At the Examiner's other cited passage where Adams' described another example system in which the privilege data selector is separate from the subscriber unit, Adams makes no mention of a website. Without some specific teaching by Adams that the subscriber unit obtains the address to the centralized privilege data from a service

advertisement, Adams cannot be said to anticipate a client obtaining a service advertisement for a service, where the service advertisement includes an address for an authentication service, as recited by Applicants' claim.

Adams clearly fails to disclose the client obtaining a service advertisement for the first service before accessing the first service, where the service advertisement includes an address for the authentication service and an address for the first service. Thus, the rejection of claim 13 is not supported by the cited art and removal thereof is respectfully requested.

Regarding claim 17, Adams fails to disclose a client obtaining a service advertisement for a service, where the service advertisement includes an address for an authentication service. The Examiner cites column 6, lines 31-67. However, the cited passage makes no mention of a client obtaining a service advertisement that includes an address for an authentication service. Instead, the cited passage describes one embodiment of Adams' system in which the relying party sends privilege test criteria data to a centralized privilege data selector and in which a subscriber sends identification information to the centralized privilege data selector. The data selector then returns to the subscriber all attribute certificates from a certificate repository that meet the received test criteria data. The subscriber then transmits the returned certificates to the relying unit. No mention is made in the cited passage regarding a client obtaining a service advertisement for a service, where the service advertisement includes an address for an authentication service. According to the Examiner's interpretation, Adams' subscriber would have to obtain a service advertisement for the relying party unit and the service advertisement would have to include an address for the centralized privilege data selector. However, Adams system does not include any service advertisement for a relying party unit that includes an address for the centralized privilege data selector. The Examiner has clearly misinterpreted the teachings of Adams.

In the Examiner's Answer, the Examiner also cites column 5, lines 14 – 17 referring to the fact that a user in Adams' system may use a website of the relying party.

The Examiner also asserts, "in order for the subscriber to request authentication credential, the subscriber must be informed of the authentication service's address as well as the first service's address." Thus, the Examiner's reasoning is that since Adams' subscriber sends a privilege verification request to the privilege data selector the website must include the address of the privilege data selector. **However, the teachings of Adams do not support the Examiner's conclusion.** Instead, the Examiner is merely speculating regarding the workings of Adams' system.

As described above regarding claim 2, Adams states, at the Examiner's cited passage, that the subscriber unit may communicate a request to a website of the relying party, which the Examiner equates to the service of Applicants' claim, to request "access to another application controlled by the relying party" (Adams, column 5, lines 13-17). Adams does not mention anything about the website including an address for the privilege data selector, which the Examiner equates to the authentication service of Applicants' claims. The cited passage that mentions the website is part of a larger passage describing as example system in which the privilege data selector is actually on the subscriber unit. For instance, Adams states, "subscriber unit 200, such as a software application, network node, or other suitable mechanism for communicating with another subscriber of relying party, *has a privilege data selector 104* in the form of an attribute certificate selector 202" (italics added, Adams, column 4, lines 58 – 62). Thus, in the example system described by Adams at the Examiner's cited passage, the privilege data selector is part of the subscriber unit. Thus, the subscriber unit would not require an address for the privilege data selector to be included in the website relied upon by the Examiner. Additionally, it would not make any sense for the "website of the relying party" to include an address for a privilege data selector on the subscriber unit.

At the Examiner's other cited passage where Adams' described another example system in which the privilege data selector is separate from the subscriber unit, Adams makes no mention of a website. Without some specific teaching by Adams that the subscriber unit obtains the address to the centralized privilege data from a service advertisement, Adams cannot be said to anticipate a client obtaining a service

advertisement for a service, where the service advertisement includes an address for an authentication service, as recited by Applicants' claim.

Adams further fails to disclose the client generating a message gate for accessing the service, where the message gate embeds the authentication credential in *every* message from the client to the service. The Examiner cites column 6, lines 65-67 where Adams states that any matching attribute certificates are sent as pre-qualification privilege data back to the subscriber unit and that the subscriber unit then transmits the pre-qualification privilege data to the relying unit through a suitable communication link. The cited passage does not mention anything about the subscriber unit, which the Examiner considered a client, generating a message gate that embeds the authentication credential in every message from the client to the service. The mere mention of "a suitable communication link" does not disclose the specific limitation of generating a message gate that embeds an authentication credential in every message. Adams does not describe, either at the cited passage or elsewhere, anything about message gates or embedding an authentication credential in every message from a client to a service. The Examiner is merely relying upon speculation, which is clearly improper.

In the Examiner's Answer, the Examiner also cites column 4, lines 10-11 and column 6, line 67 – column 7, line 2. At the first cited passage (column 4, lines 10-11) Adams states that his FIG. 1 illustrates "an example of a system for granting security privilege 100 that may be applied to a communication system employing cryptography based security." The second cited passage (column 6, line 67 – column 7, line 2) Adams states that the subscriber unit transmits the pre-qualified attributes or privilege data to the relying party unit through a suitable communication link. The Examiner argues, "[s]ince the communication is encrypted and the pre-qualification privilege data [is] transmitted to the relying party when requesting a service, thus a message gate is generated and the authentication credential [is] included in each message to the first serviced." **However, the fact that the subscriber unit sends the pre-qualification privilege data to the relying unit does not imply that the pre-qualification privilege data, which the Examiner equates with the authentication credential of Applicants' claim, is**

embedded *with every message* from the subscriber unit to the relying unit. Adams' system involves using privilege data as part of granting the subscriber unit access to some other application on the relying party. For example, Adams states that after a subscriber unit is granted privilege, "[t]he subscriber unit may then access the relying party". Thus, Adams' subscriber unit clearly sends other messages to the relying party. However, Adams does not that the pre-qualification privilege data is embedded *in every message* sent from the subscriber unit to the relying unit.

Thus, for at least the reasons above, the rejection of claim 17 is not supported by the cited art and removal thereof is respectfully requested. Similar remarks also apply to claims 58 and 69.

Regarding claim 20, Adams does not disclose the first service using the authentication service to determine if the authentication credential received in a first message from the client is authentic. The Examiner cites column 6, lines 17-20 and refers to Adams' relying unit sending test criteria data to the subscriber unit. However, the cited passage is not described the relying unit, which the Examiner equates to the first service of Applicants' claim, using the centralized privilege data selector, which the Examiner equates to the authentication service of Applicants' claim, to determine if an authentication credential received in a message from a client is authentic. Instead, the cited passage describes a subscriber unit requesting privilege test criteria data, which Adams describes as indicating the privilege data the relying unit would accept or consider, from the relying unit. In fact, in the very next sentence Adams states, "[i]t should be recognized that the subscriber unit 400 need not be authenticated by the relying party unit." Thus, the cited passage clearly fails to disclose the first service using the authentication service to determine if the authentication credential received in a message from the client is authentic.

In the Examiner's Answer, the Examiner cites column 6, line 61 to column 7, line 9 and refers to Adams' pre-qualification privilege data being generated by the authentication service/centralized privilege data selector "so that it can be verified by the

first service/relying party." The Examiner further asserts, "thus, the first service uses the authentication service to authenticate subscribers based [ ] to grant[ing] access to subscribers." **However, as noted above, Adams' relying unit receives the pre-qualification privilege data from the centralized privilege data selector and then *compares the test criteria data with the pre-qualification privilege data* as a pre-qualification privilege verification, which the Examiner considers authenticating an authentication credential. However, Adams clearly teaches that the relying unit performs this comparison on its own. Thus, the relying unit only receives the pre-qualification privilege data from the privilege data selector. It does not use the privilege data selector to perform the pre-qualification privilege verification, which the Examiner considers authenticating an authentication credential.**

Moreover, even when Adams' relying unit determines whether the pre-qualification privilege data it receives from a subscriber unit is correct, it does not involve the relying unit using the centralized privilege data selector, which the Examiner equates to an authentication service. Instead, the relying unit compares the pre-qualification privilege data it receives to its own privilege test criteria data to ensure it matches (Adams, column 6, lines 25-30 and column 7, lines 5-9).

Thus, for at least the reasons above, the rejection of claim 20 is not supported by the cited art and removal thereof is respectfully requested.

Regarding claim 21, Adams fails to disclose where the first service responds to a request message from the client only if the request message is for an authorized capability for the client. The Examiner cites column 7, lines 3-8. However, the cited passage fails to describe the relying unit responding to a request message from the client *only if the request message is for an authorized capability for the client.* Adams teaches that the relying unit sends a confirmation message "indicating whether the relying party has granted privilege to the subscriber unit" (Adams, column 6, lines 25-30). Thus, the relying unit responds to the message (with a confirmation message) whether or not the request message is for an authorized capability for the client. The relying unit may not

grant the subscriber unit privilege, but Adams' clearly teaches that it responds with a confirmation message.

In the Examiner's Answer, the Examiner argues that the "definition of 'responds' interpreted by the examiner is when access is granted". However, such an interpretation is not supported by Adams. As noted above, Adams clearly describes the relying unit *responding* to a request from the subscriber unit by sending a confirmation message indicating whether the relying has granted privilege to the subscriber unit. Thus, Adams clearly teaches that the relying unit, which the Examiner equates to the service of Applicants' claims, responds to requests regardless of whether the request is for an authorized capability for the client.

Thus, the rejection of claim 21 is not supported by the cited art and removal thereof is respectfully requested.

The rejection of claim 23 is improper because claim 23 is rejected under 35 U.S.C. § 102(a) as being anticipated by Adams but the Examiner admits in the rejection that "Adams does not explicitly disclose said first service noting whether or not said authentication credential is authentic so that said first service does not need to repeat said using said authentication service to determine if said authentication credential received in a first message from a client is authentic." **Thus, the Examiner admits that Adams fails to anticipate claim 23.** The Examiner further argues that since Single-Sign-On is well known in the art, "it would have been obvious" to allow the system to note whether the authentication credential is authentic to avoid repeating the authentication process. Firstly, the Examiner is making an obviousness-type rejection, which is improper rejection under 35 U.S.C. § 102(a). Secondly, the Examiner merely states a broad conclusion that Single-Sign-On is well known, without providing any supporting evidence to show that Single-Sign-On discloses the limitations of claim 23 nor that Single-Sign-On was well known at the time Applicants' invention was made.

In the Examiner's Answer, The Examiner states, "Adams might not have explicitly disclosed the limitation of claim 23, but Adams inherently discloses that the Single-Sign-On can be applied for services controlled by the same relying party." However, Adams makes no mention of Single-Sign-On. The Examiner does not cite any portion of Adams where Single-Sign-On is inherently disclosed. Instead, the Examiner merely states that Single-Sign-On is well-known and that Adams inherently discloses that Single-Sign-On can be applied for services controlled by the same relying party. The Examiner is incorrect and his assertions are not supported by any evidence of record.

Furthermore, as the Examiner is surely aware, "[t]o serve as an anticipation when the reference is silent about the asserted inherent characteristic, such gap in the reference may be filled with recourse to extrinsic evidence" and that "[s]uch evidence **must make clear that the missing descriptive matter is necessarily present** in the thing described n the reference, and that it would be so recognized by persons of ordinary skill" (emphasis added, M.P.E.P. § 2131.01 III). The Examiner has not provided any such extrinsic evidence. Instead, the Examiner has merely stated that Adams inherently discloses Single-Sign-On. Thus, without some extrinsic evidence showing that Single-Sign-On is ***necessarily*** present in Adams' system, Adams clearly fails to anticipate claim 23.

Thus, the rejection of claim 23 is clearly improper and not supported by the cited art. Removal of the rejection of claim 23 is respectfully requested.

Regarding claim 24, Adams fails to disclose a service advertisement for the first service that includes an address for accessing the first service. The Examiner cites column 6, lines 31-41. However, this passage makes no mention of any service advertisement for the first service that includes an address for accessing the first service. As described previously, the cited passage describes Adams' centralized privilege data selector. Nowhere does Adams describe any sort of service advertisement including an address for the service. The Examiner fails to cite and portion of Adams or provide any

interpretation of Adams' teachings that disclose a service advertisement for the first service that includes an address for accessing the first service.

In the Examiner's Answer the Examiner again refers to column 5, lines 14 – 17 and column 6, lines 49-51 of Adams. The Examiner also asserts, "in order for the subscriber to request authentication credential, the subscriber must be informed of the authentication service's address as well as the first service's address." **However, claim 24 recites that the service advertisement includes an address *for accessing the first service.* Thus, the Examiner's assertion regarding how the subscriber must be informed of the authentication service's address is irrelevant.**

Thus, the rejection of claim 24 is not supported by the cited art and removal thereof is respectfully requested.

Section 103(a) Rejection:

The Examiner rejected claims 3-6, 18, 19, 29-31, 44-45, 52, 53, 55, 64 and 65 under 35 U.S.C. § 103(a) as being unpatentable over Adams in view of Czerwinski, et al. ("An Architecture for a Secure Service Discovery Service") (hereinafter "Czerwinski"). Applicants respectfully traverse this rejection for at least the reasons below.

Regarding claim 3, Adams in view of Czerwinski fails to teach or suggest that the advertisement for the first service includes a data representation language schema *defining a message interface* for accessing the first service. The Examiner admits that Adams fails to teach or suggest an advertisement for the first service that includes a data representation language schema defining a message interface for accessing the first service and relies upon Czerwinski. However, Czerwinski does not teach that the advertisement for the first service includes a data representation language schema *defining a message interface* for accessing the first service. In contrast, Czerwinski discloses domain advertisements that contain "the multicast address to use for sending service announcements, the desired service announcement rate, and contact information

for the Certificate Authority and the Capability Manager" (Czerwinski, section 3.1, paragraph 1). Additionally, Czerwinski's service descriptions contain service metadata, such as location, required capabilities, time-out period, and JAVA RMI addresses (Czerwinski, section 2.3, paragraph 3). Neither the domain advertisements nor the service descriptions of Czerwinski include a data representation language schema defining a message interface for accessing a service.

Furthermore, no combination of Adams and Czerwinski teaches or suggests that the advertisement for the first service includes a data representation language schema *defining a message interface* for accessing the first service. Thus, the rejection of claim 3 is not supported by the cited art and removal thereof is respectfully requested.

Regarding claim 4, Adams in view of Czerwinski fails to teach or suggest that the first message, sent from the client to the service and including the authentication credential, corresponds to a message defined in the data representation language schema. The Examiner admits that Adams fails to teach the limitations of claim 4 and relies upon Czerwinski, citing Czerwinski's teachings regarding XML queries. The Examiner cites a portion of Czerwinski (section 3.1) that describes how a client submits a query in the form of an XML template. However, a client query using an XML template as the content of a query is very different from a data representation language schema defining a message interface for accessing a service. The XML template in a client query in Czerwinski does not define a message interface for accessing a service. Instead client queries include desired services and are matched against service descriptions to find services providing those desired services (Czerwinski, section 2.3, paragraph 3 and section 3.1, paragraph 5). Further, Czerwinski teaches the use of Authenticated Remote Method Invocation (ARMI) for communication between client applications and SDS servers, *and it is well known that ARMI uses Java interface classes, and not data representation language schemas*, to define the methods that are exposed for remote calling. Thus, Czerwinski clearly fails to teach wherein the advertisement for the first service includes a data representation language schema defining a message interface for accessing the first service. Thus, a client query in Czerwinski is not a data representation

schema, and does not define a message interface for accessing a service. As noted above, there is no way in Czerwinski for a client to define such a message interface in a query template when the client has not even located a service (that is purpose of submitting the query template) and it would be impossible in Czerwinski for the client to define a message interface for a service that has not even been located and/or selected.

Furthermore, Czerwinski teaches the use of Authenticated Remote Method Invocation (ARMI) for communication between client applications and SDS servers, *and it is well known that ARMI uses Java interface classes, not data representation language schemas*, to define the methods that are exposed for remote calling. Thus, the clients do not use messages defined in data representation language schemas in Czerwinski's system and certainly do not use messages defined in data representation language schema for submitting queries to SDS servers.

Thus, the combination of Adams and Czerwinski clearly fails to teach or suggest that the first message, sent from the client to the service and including the authentication credential, corresponds to a message defined in the data representation language schema.

Regarding claim 5, Adams in view of Czerwinski fails to teach or suggest the client sending additional messages to the service to use the service wherein the authentication credential is included with each one of the additional messages. The Examiner cites column 6, lines 31 – 67 of Adams. However, Adams does not mention anything regarding including an authentication credential with each additional message sent by the client to the service. Adams only states that the subscriber unit transmits the pre-qualification attributes or privilege data to the relying unit "through a suitable communication link" (Adams, column 6, line 67 – column 7, line 2). Adams fails to mention anything regarding the sending of additional message or about an authentication credential included in each of the additional messages.

Czerwinski also fails to teach or suggest the client sending additional messages to the service to use the service wherein the authentication credential is included with each one of the additional messages. Czerwinski teaches that authentication in ARMI "consists of a short handshake that establishes a symmetric [encryption] key used for the rest of the session" and that "ARMI uses certificates to authenticate each of the endpoints" (Czerwinski, page 28, section 3.5.3). Thus, Czerwinski teaches performing a handshake once at the beginning of a session in which certificates are used to authenticate each endpoint and the symmetric encryption key is used for the remainder of the session. Czerwinski does not mention including an authentication credential with each additional message. Even if combined, Adams and Czerwinski fail to teach or suggest the client sending additional messages to the service to use the service wherein the authentication credential is included with each one of the additional messages.

Furthermore, since any additional messages (after the initial handshake) are encrypted and decrypted using the symmetric encryption key, there is not need to include any authentication credential with each message. Hence, **Czerwinski teaches away** from an authentication credential included with each one of the additional messages.

Adams in view of Czerwinski also fails to teach or suggest wherein each one of the additional messages is defined by the data representation language schema. The Examiner cites Czerwinski's teachings regarding XML queries. However, as noted above, regarding the rejection of claims 3 and 4, Czerwinski fails to teach sending message that are defined by a data representation language schema. Thus, Czerwinski clearly fails to teach sending additional message, where each additional message is defined by the data representation language schema. Adams fails, as admitted by the Examiner in the rejection of claim 4, to teach or suggest sending messages defined by a data representation language schema and thus, Adams fails to overcome the deficiencies of Czerwinski regarding sending additional messages where each additional message is defined by the data representation language schema.

Therefore the combination of Adams and Czerwinski clearly fails to teach or suggest the client sending additional messages to the service to use the service wherein the authentication credential is included with each one of the additional messages wherein each one of the additional messages is defined by the data representation language schema. The rejection of claim 5 is not supported by the cited art and removal thereof is respectfully requested.

Regarding claim 18, Adams in view of Czerwinski does not teach or suggest that the advertisement for the first service includes a data representation language schema *defining a message interface* for accessing the first service. The Examiner admits that Adams fails to teach the limitations of claim 18 and relies upon Czerwinski, citing section 2.3 and referring to Czerwinski's XML Service Description. However, the cited section does not describe a service advertisement that includes a data representation language schema defining a message interface for accessing the service. Czerwinski discloses domain advertisements that contain "the multicast address to use for sending service announcements, the desired service announcement rate, and contact information for the Certificate Authority and the Capability Manager" (Czerwinski, section 3.1, paragraph 1). Additionally, Czerwinski's service descriptions contain service metadata, such as location, required capabilities, time-out period, and JAVA RMI addresses (Czerwinski, section 2.3, paragraph 3). Neither the domain advertisements nor the service descriptions of Czerwinski include a data representation language schema defining a message interface for accessing a service. For a more detailed discussion regarding Czerwinski's failure to teach including, in a service advertisement, a data representation language schema defining a message interface for accessing a service, please see the discussion of claim 3 above.

Additionally, Adams in view of Czerwinski does not teach or suggest the message gate verifies that each message sent from the client to the first service complies with the data representation language schema. The Examiner again cites sections 3.1 of Czerwinski and refers to a client (in Czerwinski) using Authenticated RMI. However, the cited section does not mention any sort of message gate verifying that messages sent

from a client to a service comply with a data representation language schema. Please refer to the discussion of claim 14 for a more detailed discussion of Czerwinski's failure to teach a message gate that verifies that messages comply with a data representation language schema.

As neither Adams nor Czerwinski teach or suggest that the advertisement for the first service includes a data representation language schema *defining a message interface* for accessing the first service and that the message gate verifies that each message sent from the client to the first service complies with the data representation language schema, Adams and Czerwinski, whether considered singly or in combination, fail to teach or suggest the limitations of claim 18. Thus, the rejection of claim 18 is not supported by the cited art and removal thereof is respectfully requested.

Furthermore, claim 18 recites limitations similar to claim 14, which the Examiner indicates would be allowable if rewritten in independent form.

Regarding claim 29, Adams in view of Czerwinski fails to teach or suggest wherein the advertisement for the first service includes a data representation language schema defining a message interface for accessing the first service, and where the first message corresponds to a message defined in said data representation language schema. Please refer to the arguments presented above regarding claim 3 and 4, as they also apply to claim 29. Thus, for at least the reasons above, the rejection of claim 29 is not supported by the cited art and removal thereof is respectfully requested.

Regarding claim 30, Adams in view of Czerwinski fails to teach or suggest wherein said first message corresponds to a message defined in said data representation language schema. Please refer to the arguments presented above regarding claim 5, as they also apply to claim 30. Thus, for at least the reasons above, the rejection of claim 30 is not supported by the cited art and removal thereof is respectfully requested.

Regarding claim 44, Adams in view of Czerwinski fails to teach or suggest wherein the advertisement for the first service includes a data representation language schema defining a message interface for accessing the first service. Please refer to the arguments presented above regarding claim 3, as they also apply to claim 44. Thus, for at least the reasons above, the rejection of claim 44 is not supported by the cited art and removal thereof is respectfully requested.

Regarding claim 45, Adams in view of Czerwinski fails to teach or suggest wherein said first message corresponds to a message defined in said data representation language schema. Please refer to the arguments presented above regarding claim 5, as they also apply to claim 45. Thus, for at least the reasons above, the rejection of claim 45 is not supported by the cited art and removal thereof is respectfully requested.

Regarding claim 52, Adams in view of Czerwinski fails to teach or suggest a client obtaining an address for the authentication service from an advertisement for the service, wherein accessing the authentication service includes the client sending a message to the address for the authentication service requesting the authentication credential to use the advertised service. The Examiner cites FIG. 5 and column 6, lines 31-40 of Adams. However, the cited portions make no mention of a client obtaining an address for the authentication service from an advertisement for the service. Instead, the cited passage describes one embodiment of Adams' system in which the relying party sends privilege test criteria data to a centralized privilege data selector and in which a subscriber sends identification information to the centralized privilege data selector. The data selector then returns to the subscriber all attribute certificates from a certificate repository that meet the received test criteria data. The subscriber then transmits the returned certificates to the relying unit. Nowhere does Adams describe a client obtaining an address for the authentication service from an advertisement for the service.

Czerwinski, not relied upon by the Examiner, also fails to teach or suggest a client obtaining an address for the authentication service from an advertisement for the service, wherein accessing the authentication service includes the client sending a message to the

address for the authentication service requesting the authentication credential to use the advertised service. Thus, Czerwinski fails to over the above noted deficiencies of Adams.

Adams in view of Czerwinski further fails to teach or suggest that the advertisement for the first service includes a data representation language schema *defining a message interface* for accessing the first service. The Examiner admits that Adams fails to teach or suggest an advertisement for the first service that includes a data representation language schema defining a message interface for accessing the first service and relies upon Czerwinski. However, Czerwinski does not teach that the advertisement for the first service includes a data representation language schema *defining a message interface* for accessing the first service. In contrast, Czerwinski discloses domain advertisements that contain "the multicast address to use for sending service announcements, the desired service announcement rate, and contact information for the Certificate Authority and the Capability Manager" (Czerwinski, section 3.1, paragraph 1). Additionally, Czerwinski's service descriptions contain service metadata, such as location, required capabilities, time-out period, and JAVA RMI addresses (Czerwinski, section 2.3, paragraph 3). Neither the domain advertisements nor the service descriptions of Czerwinski include a data representation language schema defining a message interface for accessing a service.

Furthermore, no combination of Adams and Czerwinski teaches or suggests a client obtaining an address for the authentication service from an advertisement for the service, wherein accessing the authentication service includes the client sending a message to the address for the authentication service requesting the authentication credential to use the advertised service and that the advertisement for the first service includes a data representation language schema *defining a message interface* for accessing the first service. Thus, the rejection of claim 52 is not supported by the cited art and removal thereof is respectfully requested.

Regarding claim 53, Adams in view of Czerwinski fails to teach or suggest wherein the advertisement for the first service includes a data representation language schema defining a message interface for accessing the first service, and where the first message corresponds to a message defined in said data representation language schema. Please refer to the arguments presented above regarding claims 3 and 4, as they also apply to claim 53. Thus, for at least the reasons above, the rejection of claim 53 is not supported by the cited art and removal thereof is respectfully requested.

Regarding claim 64, Adams in view of Czerwinski fails to teach or suggest wherein the advertisement for the first service includes a data representation language schema defining a message interface for accessing the first service, and where the first message corresponds to a message defined in said data representation language schema. Please refer to the arguments presented above regarding claims 3 and 4, as they also apply to claim 64. Thus, for at least the reasons above, the rejection of claim 64 is not supported by the cited art and removal thereof is respectfully requested.

CONCLUSION

Applicants submit the application is in condition for allowance, and prompt notice to that effect is respectfully requested.

If any extension of time (under 37 C.F.R. § 1.136) is necessary to prevent the above-referenced application from becoming abandoned, Applicants hereby petition for such an extension. If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5181-64800/RCK.

Also enclosed herewith are the following items:

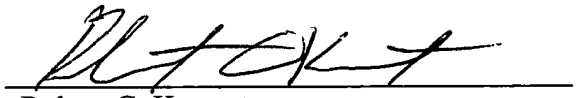
☒ Return Receipt Postcard

☐ Petition for Extension of Time

☐ Notice of Change of Address

☐ Other:

Respectfully submitted,



Robert C. Kowert
Reg. No. 39,255
ATTORNEY FOR APPLICANT(S)

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: October 11, 2006